REMARKS/ARGUMENTS

The Examiner is thanked for the clarity and conciseness of the previous Office Action, and for the citation of references, which have been studied with interest and care.

In the Office Action, the Examiner contends that Applicant claims two distinct inventions in the above-identified United States Patent Application; namely, I. Claims 1-26 and 33-46, drawn to a system to identify a device, classified in class 726, subclass 7 and II. Claims 27-32, drawn to a system to identify a user, classified in class 713, subclass 182.

Thus, pursuant to 35 U.S.C. § 121, the Examiner has required Applicant to restrict the Application to one of the alleged two inventions.

Applicant acknowledges that an oral election was made to the restriction requirement, in which Applicant elected Group I and Species III which relate to claims 1-4, 9-17, 22-26, 33-37, and 42-46 without traverse. Accordingly, Applicant has withdrawn claims 5-8, 18-21, and 27-32.

In the Office Action, claims 1-4, 9-17, 22-26, 33-37, and 42-46 stand rejected under 35 U.S.C. § 103.

Applicant has canceled dependent claims 2 and 15 and has re-written the limitations into independent claims 1 and 14, respectively, to further clarify the embodiments of the invention. Additionally, Applicant has canceled claims 33-46 without prejudice.

Reconsideration in light of the amendments and remarks made herein is respectfully requested.

Rejection Under 35 U.S.C. § 103

Claims 1-4, 9-17, 22-26, 33-37, and 42-46 stand rejected under 35 U.S.C. § 103(a) as being allegedly rendered obvious by The Handbook of Applied Cryptography authored by Menezes et al. (hereinafter Menezes) in view of U.S. Patent No. 4,817,140 issued to Chandra (hereinafter Chandra).

Applicant respectfully traverses the Office Action's §103 obviousness rejections in their entirety, in light of the following remarks. As stated in MPEP §2141.03:

> A prima facie obviousness rejection requires the three basic criteria be met. First, there must be some teaching, suggestion, or motivation, either in the references of themselves, or in the knowledge generally available to one skilled in the art, to modify the reference or to combine the references. Second, there must be some reasonable expectation of success. Finally, the prior art reference, or references when combined, *must teach all the claim limitations.* The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, *and not based on the Applicant's disclosure*. MPEP §2141.03. (Emphasis added).

Applicant respectfully submits that the Office Action has misconstrued the teachings of Menezes and Chandra, and even if they were properly combinable, their combination would still not teach or suggest the claim limitations of Applicant's amended independent claims 1 and 14.

Particularly, amended independent claims 1 and 14 include limitations generally directed to a system and method to uniquely identify a security device, the security device coupled to a computing device, in which the computing device is coupled to a server over a network...including functionality related to: *storing a serial number associated with the security device and a user key associated with the serial number that is unique to the security device in a secure memory of the security device...storing a plurality of registered serial numbers and a plurality of user keys at the server, where each user key is associated with one of the plurality of registered serial numbers*...requesting a serial number from the security device when the computing device *attempts to log on to the server over the computer network*...verifying whether the serial number received from the security device is stored as one of the plurality of registered serial numbers at the server...and if the serial number is stored at the server, obtaining the associated user key from the server, computing a challenge, computing an expected response based on the associated user key, sending the challenge to the security device over the computer network, and, *if the server receives the response back from the security device in response to the challenge that matches the expected response, allowing the computing device to log on to the server.*

The Office Action cites Menezes because Menezes teaches mathematics associated with cryptographic challenge-response identification utilizing keys.

However, Applicant respectfully submits that nowhere does Menezes teach or suggest a *security device coupled to a computing device*, the computing device coupled to a server over a computer network...and techniques comprising...*storing a serial number associated with the security device and a user key associated with the serial number that is unique to the security device in the secure memory of the security device...storing a plurality of registered serial numbers and a plurality of user keys at the server, wherein each user key is associated with one of the plurality of registered serial numbers*...requesting a serial number from the security device when the computing device attempts to log on to the server over the computer network...verifying whether the serial number received from the security device is stored as one of the plurality of registered serial numbers at the server...and if the serial number is stored at the server implementing a challenge-response such that if the server receives a response back from the security device in response to the challenge that matches the expected response, allowing the computing device to log on to the server.

In fact, on page 4 of the Office Action, the Office Action explicitly recognizes that Menezes does not disclose a security device coupled to a computer.

Particularly, nowhere does Menezes teach or suggest a security device coupled to a computing device in which the computing device is coupled to a server over a computer network or a security device storing a serial number associated with the security device and a user key associated with the serial number that is unique to the security device in a secured memory, nor does Menezes teach or suggest the other limitations associated with Applicant's independent claims 1 and 14.

Applicant respectfully submits that Menezes is simply cited for teaching the mathematics associated with a cryptographic challenge-response protocol and does not teach any of the above-described claim limitations of Applicant's amended independent claims 1 and 14.

In order to recreate Applicant's claimed invention in hindsight, the Office Action attempts to combine Menezes with Chandra. However, Applicant respectfully submits that even if these references were properly combinable, they still would not teach or suggest the limitations of Applicant's independent claims 1 and 14.

As set forth in the Abstract of Chandra, Chandra relates to a software asset protection mechanism which is based on the separation of software to be protected from the right to execute that software...in which...protected software can only be executed on composite computing systems in which a physically and logically secure co-processor is associated with a host computer...The software being protected is broken down into a protected (encrypted) portion and an (optional) unprotected or plain text portion...The software is distributed by any conventional software distribution mechanism (for example a floppy disk) including the files already identified along with an encrypted software decryption key...The coprocessor is capable of decrypting the software decryption key so it can thereafter decrypt the software, for execution purposes...However, the coprocessor will not perform these functions unless and until the *user's right to execute is evidenced by presence of a physically secure token.* The physically secure token provides to the coprocessor token data in plain text form (the physical security of the plain text token data is provided by the cartridge within which token data is stored)...(Abstract, emphasis added).

As set forth above in the Abstract, Chandra is related to a very different invention. Particularly, nowhere does Chandra teach or suggest a *computing device coupled to a server over a computer network*...in which a security device is coupled to the computing device and *the security device stores a serial number associated with the security device and a user key associated with the serial number that is unique to the security device in a secure memory...storing a plurality of registered serial numbers and a plurality of user keys at the server in which each user key is associated with one of the plurality of registered serial numbers* and verifying whether a serial number received from the security device is stored as one of the plurality of registered serial numbers at the server and then performing a challenge-response...and *if the server receives a response back from the security device and response to*

the challenge that matches the expected response, allowing the computing device to log on to the server.

Applicant respectfully submits that nowhere are these claim limitations taught in the proposed combination of Menezes and Chandra.

Of particular note, in rejecting dependent claims 2 and 15, now re-written into independent claims 1 and 14, the Office Action stated that Chandra discloses keys that are stored in the secure memory and cites column 11, lines 55-59.

However, column 11, lines 55-59 of Chandra teach that: "The second privilege level includes the key management functions of acquiring a right to execute and, once acquired, copying the necessary decryption key into the secure memory space (second privilege level) of the coprocessor." (Emphasis added)

Continuing on, in column 11, Chandra further states that: "As distributed, of course, the protected software is inexecutable by the host computer as at least a portion is encrypted...the software is executable by the coprocessor once it has authorization by the second privilege level...the further tangible element is the hardware cartridge storing the transfer token..." (Emphasis added)

In a more detailed explanation of this, Chandra explains that to: "[D]ecrypt the encrypted portion of the protected software, the coprocessor must be provided with the decryption key...needed to render the encrypted portion of software executable...The (decryption) key must be transferred to the software owner's coprocessor in such a way that the transfer mechanism cannot be reused or reproduced by a user and thus grant key transfer to other personal computers...This is accomplished by associating the effective transfer of the decryption key into the non-volatile memory of the coprocessor with a transaction token, e.g. the presence of the transaction token is required to effectively transfer the decryption key to the coprocessor." (Column 4, lines 1-15). (Emphasis added)

Thus, although Chandra does disclose a coprocessor that has a non-volatile memory, it is directed to a process requiring a transaction token to transfer a decryption key into a non-volatile memory of the coprocessor.

Column 19, lines 60-68 and Column 20 lines 1-25 of Chandra describe the type of token cartridge that is utilized to transfer this decryption key in to the nonvolatile memory of the coprocessor. Chandra describes a type of token cartridge that cannot be reused or reproduced such that it is only useable once to transfer the decryption key for the particular software to the non-volatile memory of the coprocessor.

All of this is done for the purpose of obtaining a decryption key that can be stored in non-volatile memory for the purpose of decrypting and executing a particular software program.

In contrast the Office Action's assertion, this is no way teaches or suggests Applicant's claims related to *storing a serial number associated with the security device and a user key associated with the serial number that is unique to the security device in a secure memory* wherein Applicant's user key is unique to the security device and is used in a challenge-response (along with the serial number) in order to identify the security device.

Quite simply neither Mendez and Chandra teach or suggest the use of a security device coupled to a computing device in turn coupled to a server over a computer network, or the use a serial number and a user key associated associated with the serial number that is unique to the security device (both stored in a secure memory of the security device), a server that stores matching user keys, etc., for use in a challenge-response to authenticate a security device to allow a computer to log onto a server.

More particularly, Applicant respectfully submits that teachings of Chandra, even if they were properly combinable with Menezes, would still in no way teach or suggest a *computing device coupled to a server over a computer network*...in which a security device is coupled to the computing device and *the security device stores a serial number associated with the security device and a user key associated with the serial number that is unique to the security device in a secure memory*...*storing a plurality of registered serial numbers and a plurality of user keys at*

the server in which each user key is associated with one of the plurality of registered serial numbers and verifying whether a serial number received from the security device is stored as one of the plurality of registered serial numbers at the server and then performing a challenge-response...and *if the server receives a response back from the security device and response to the challenge that matches the expected response, allowing the computing device to log on to the server.*

Applicant respectfully submits that Chandra is related to a totally different invention and that the combination of Menezes with Chandra does not teach or suggest the limitations of Applicant's independent claims 1 and 14, and that these claims should be allowable. Further, Applicant respectfully submits that the claims that depend therefrom should also be allowable. Applicant respectfully requests that the Examiner allow these claims and move the case to issuance.

Conclusion

In view of the remarks made above, it is respectfully submitted that pending claims 1-46 define the subject invention over the prior art of record. Thus, Applicant respectfully submits that all the pending claims are in condition for allowance, and such action is earnestly solicited at the earliest possible date. The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application. To the extent necessary, a petition for an extension of time under 37 C.F.R. is hereby made. Please charge any shortage in fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 3/17/2006 By _____

Eric T King
Reg. No. 44,188
Tel.: (714) 557-3800 (Pacific Coast)

Attachments

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☒ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: 3/17/2006

FACSIMILE

☐ *transmitted by facsimile to the Patent and Trademark Office.*

Nicole Erquiaga 3/17/2006
Date